UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,889	12/07/2005	Junbiao Zhang	PU030227	2851

24498 7590 06/21/2010

Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

EXAMINER	
NGUYEN, TRONG H	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
06/21/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/559,889	ZHANG ET AL.	
	Examiner	Art Unit	
	TRONG NGUYEN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 03/04/2010. In response to the office action mailed on 12/04/2009, claims 1, 4, 10 and 11 have been amended. Pending claims include **claims 1 and 3-14**.

The objection to claims 10-11 has been withdrawn due to Applicants' amendments.

The rejection of claim 4 under 35 USC 112, second paragraph has been withdrawn due to Applicants' amendment.

Response to Arguments

2. Applicants' arguments filed 03/04/2010 have been fully considered but the following argument(s) is/are not persuasive.

Applicants argue that:

i. The combination of Lewis and Jordan is inappropriate because Jordan does not teach or suggest any device that even remotely resembles an access point. Jordan shows a system in Figure 1, which lacks a device called or resembling a wireless access point. Although it has been suggested in the Office Action that the messaging gateway 115 of Jordan is analogous to Applicants' access point, the analogy fails because the messaging gateway of Lewis is not in communication with any user. Jordan's messaging gateway 115 is separated from the user (i.e., Jordan's wireless devices 130 or 135) by a number of different system devices. These different system devices are interposed along the communication path from the user and the gateway so

that the user is not in direct communication with the gateway. Applicants call at least for "communicating the newly generated encryption key from the access point directly to the station in an encrypted form using the old encryption key", as defined in claim 1 and shown in Applicants' Figure 1. Jordan's only shows a communications tower 125 and a loader 175 directly communicating with the two different wireless devices. If Jordan's messaging gateway is intended to be analogous to an access point, then it fails to teach or suggest Applicants' claimed limitation.

In response to applicants' arguments:

i. The examiner respectfully disagrees for the following reasons. Although Jordan uses the example of synchronizing password keys between a messaging gateway and a wireless device, Jordan's synchronization methods are not limited to only this example. Jordan specifically states that other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims (par. 0115). In addition, Jordan discloses that the wireless communication system shown in Fig. 1 is an exemplary embodiment of a wireless communication system in which Jordan's synchronization methods may be implemented (pars. 0033-0034). Thus, one of ordinary skill in the art would readily recognize that Jordan's synchronization methods can be implemented in other wireless communication systems where there is a need to maintain secure wireless

transmissions including a wireless communication system comprising access points and stations.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

"the number" on line 2 lacks antecedent basis.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 7-8 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. US 2003/0221098 A1 (hereinafter "Chen") in view of Jordan et al. US 2004/0081320 A1 (hereinafter "Jordan").

Regarding claim 1, Chen discloses a key synchronization method for a wireless network comprising:

setting a current encryption key and an old encryption key at an access point in the wireless network; [par. 0053: The first ciphering key K1 is successfully updated into the second ciphering key K2, the access point 34 and the station P1 use the second ciphering key K2 to encrypt or decrypt the transmission data until the next time that the counting module 36 detonates the random-code generation program 38 to generate a third ciphering key K3, then repeat the above steps to update the second ciphering key K2 into the third ciphering key K3. Par. 0055: The access point 34 further comprises a memory 40 for recording the new ciphering key and all old ciphering keys. Assume that the new ciphering key of the wireless network system 30 is the third ciphering key K3. The memory 40 records the third ciphering key K3, the second ciphering key K2, and the first ciphering key K1]

generating a new encryption key at the access point; [par. 0053: The first ciphering key K1 is successfully updated into the second ciphering key K2, the access point 34 and the station P1 use the second ciphering key K2 to encrypt or decrypt the transmission data until the next time that the counting module 36 detonates the random-code generation program 38 to generate a third ciphering key K3, then repeat the above steps to update the second ciphering key K2 into the third ciphering key K3]

resetting at the access point the current encryption key to equal the newly generated encryption key; [par. 0053: The first ciphering key K1 is successfully updated into the second ciphering key K2, the access point 34 and the station P1 use the second ciphering key K2 to encrypt or decrypt the transmission data until the next time that the counting module 36 detonates the random-code generation program 38 to

generate a third ciphering key K3, then repeat the above steps to update the second ciphering key K2 into the third ciphering key K3]

resetting at the access point the old encryption key to equal an encryption key being used by a station in communication with the access point; [par. 0043: After receiving the agreement response transmitted from the station P1, the access point 34 uses the first ciphering key K1 (in this case, the second ciphering key K2) to encrypt the second ciphering key K2 (in this case, the third ciphering key K3) and then transmits the encrypted second ciphering key K2 (in this case, the encrypted third ciphering key K3) to the station P1]

communicating the newly generated encryption key from the access point directly to the station in an encrypted form using the old encryption key; [par. 0043: After receiving the agreement response transmitted from the station P1, the access point 34 uses the first ciphering key K1 (in this case, the second ciphering key K2) to encrypt the second ciphering key K2 (in this case, the third ciphering key K3) and then transmits the encrypted second ciphering key K2 (in this case, the encrypted third ciphering key K3) to the station P1]

indicating at the access point a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key, [Fig. 3 and par. 0051: The access point 34 also uses the second ciphering key K2 (in this case, the third ciphering key K3) to encrypt the confirmation challenge text into a confirmation standard text; after receiving the confirmation response text transmitted from the station P1, the access point 34

compares the confirmation response text to the confirmation standard text, ...if the confirmation response text does not match the confirmation standard text, that means the station P1 has not updated the first ciphering key K1 (in this case, the second ciphering key K2) into the second ciphering key K2 (in this case, the third ciphering key K3) yet, therefore, go back to step 110]

resetting at the access point the old encryption key to equal the current encryption key when decryption using the new encryption key is successful [Par. 0053: The first ciphering key K1 (in this case, the second ciphering key K2) is successfully updated into the second ciphering key K2 (in this case, the third ciphering key K3), the access point 34 and the station P1 use the second ciphering key K2 (in this case, the third ciphering key K3) to encrypt or decrypt the transmission data until the next time that the counting module 36 detonates the random-code generation program 38 to generate a third ciphering key K3 (in this case, the fourth ciphering key K4), then repeat the above steps to update the second ciphering key K2 (in this case, the third ciphering key K3) into the third ciphering key K3 (in this case, the fourth ciphering key K4)]

Chen does not specifically disclose **wherein a data frame that failed to decrypt using the current encryption key is decrypted by said access point using the old encryption key**.

However, Jordan discloses methods of changing and synchronizing a password key in a wireless communication system when there is a transmit or receive error, the messaging gateway reverts back to a password key that is prior to the most recent

updated password key (i.e. the old encryption key) to decrypt a message received from the wireless device after unsuccessfully decrypting the message using the updated password key (i.e. the current password key) (Figs. 10-11, Pars. 0089 and 0093-0094).

Jordan and Chen are analogous art because they are in the same field of endeavor of secure data communication in a wireless communication system.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen by using the old encryption key to decrypt a data frame that failed to decrypt using the current encryption key as described by Jordan for the purpose of recovering from a transmit or receive error through resynchronization of password keys (Jordan, Par. 0087).

Regarding claim 7, Chen-Jordan combination further discloses **the method according to claim 1, wherein said setting is performed by the access point for each station in the wireless network** as [see rejection to claim **1** above and Chen's Fig. 2 and par. 0017]

Regarding claim 8, Chen discloses a key synchronization system for a wireless network comprising:

at least one station in the wireless network; [Fig. 2: a plurality of stations P1-P3]

at least one access point in the wireless network [Fig. 2: at least one access point 34] **maintaining an old encryption key and a new encryption key through a**

key rotation interval for each of said at least one station [par. 0053: The first ciphering key K1 is successfully updated into the second ciphering key K2, the access point 34 and the station P1 use the second ciphering key K2 to encrypt or decrypt the transmission data until the next time that the counting module 36 detonates the random-code generation program 38 to generate a third ciphering key K3, then repeat the above steps to update the second ciphering key K2 into the third ciphering key K3. Par. 0055: The access point 34 further comprises a memory 40 for recording the new ciphering key and all old ciphering keys. Assume that the new ciphering key of the wireless network system 30 is the third ciphering key K3. The memory 40 records the third ciphering key K3, the second ciphering key K2, and the first ciphering key K1] **said access point using said new encryption key when a first data frame correctly encrypted with said new encryption key is received from said at least one station** [if the confirmation response text matches the confirmation standard text, that means the station P1 has successfully updated the first ciphering key K1 (in this case, the second ciphering key K2) into the second ciphering key K2 (in this case, the third ciphering key K3), therefore, the follow up transmission data between the access point 34 and the station P1 is encrypted and decrypted by the second ciphering key K2 (in this case, the third ciphering key K3), therefore, continuously execute step 250] **using said old encryption key due to mismatched keys** [par. 0051: if the confirmation response text does not match the confirmation standard text, that means the station P1 has not updated the first ciphering key K1 (in this case, the second ciphering key K2) into the second ciphering key K2 (in this case, the third ciphering key K3) yet, therefore, go back

to step 110] **said access point resetting the old encryption key to equal the new encryption key when decryption with the new encryption key is successful** [Par. 0053: The first ciphering key K1 (in this case, the second ciphering key K2) is successfully updated into the second ciphering key K2 (in this case, the third ciphering key K3), the access point 34 and the station P1 use the second ciphering key K2 (in this case, the third ciphering key K3) to encrypt or decrypt the transmission data until the next time that the counting module 36 detonates the random-code generation program 38 to generate a third ciphering key K3 (in this case, the fourth ciphering key K4), then repeat the above steps to update the second ciphering key K2 (in this case, the third ciphering key K3) into the third ciphering key K3 (in this case, the fourth ciphering key K4)]

Although Chen discloses using said old encryption key due to mismatched keys, Chen does not specifically disclose when **decryption** of a data frame received from said at least one station fails.

However, Jordan discloses methods of changing and synchronizing a password key in a wireless communication system when there is a transmit or receive error, the messaging gateway reverts back to a password key that is prior to the most recent updated password key (i.e. the old encryption key) to decrypt a message received from the wireless device after unsuccessfully decrypting the message using the updated password key (i.e. the current password key) (Figs. 10-11, Pars. 0089 and 0093-0094).

Jordan and Chen are analogous art because they are in the same field of endeavor of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen by using the old encryption key when decryption of a data frame received from said at least one station fails as described by Jordan for the purpose of recovering from a transmit or receive error through resynchronization of password keys (Jordan, Par. 0087).

Regarding claim 13, Chen-Jordan combination further discloses **the method according to claim 1, wherein the new encryption key is generated at the access point upon expiration of a key refresh interval** [Chen, par. 0054: As long as the random-code generation program 38 is detonated to generate a new ciphering key each time the counting module 36 conforms to a predetermined time, it is covered by the disclosure of the present invention. In addition, the predetermined time can be a fixed time or a non-fixed time. That means the wireless network system 30 can update the common ciphering key according to a fixed time or a random time. No matter if the common ciphering key is updated according to a fixed time or a random time, the ciphering key also can be automatically updated]

6. **Claims 3, 4, 9 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen in view of Jordan and further in view of Loc et al. US 7,293,289 (hereinafter "Loc").

Regarding claim 3, Chen-Jordan combination further discloses **the method according to claim 1, further comprising: decrypting received data frames at the access point using the old encryption key** as [see rejection to claim **1** above] but does not specifically disclose the received data frames are **associated with said out-of-sync counter** and **incrementing an out-of-sync counter in the access point when said decryption failure occurs due to the encryption key used by the station not matching the current encryption key**.

However, Loc discloses a method for detecting a security breach in a network wherein "Each time a client 108 fails to successfully decrypt a packet, the encryption failure counter is incremented" (Fig. 5, Col. 6, lines 59-61). Furthermore, Jordan discloses that when there is a transmit or receive error, the messaging gateway reverts back to a password key that is prior to the most recent updated password key (i.e. the old encryption key) to decrypt a message received from the wireless device after unsuccessfully decrypting the message using the updated password key (i.e. the current password key) (Figs. 10-11, Pars. 0089 and 0093).

Loc, Chen, and Jordan are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen-Jordan by incrementing an out-of-sync counter in the access point when said decryption failure occurs due to the encryption key used by the station not matching the current encryption key and decrypting received data frames associated with said out-of-sync counter as described by Loc in order to

detect a security breach in a network (Loc, Col. 1, lines 22-23) and resynchronizing password keys (Jordan, Par. 0087).

Regarding claim 4, Chen-Jordan combination further discloses **the method according to claim 1, further comprising:**

decrypting, using the new encryption key, the received data frame from the station when the access point determines the station sending the received data frame is using the new encryption key, said access point starting to use the new encryption key when a first data frame correctly encrypted with the new encryption key is received from the station; as [Chen, par. 0051: if the confirmation response text matches the confirmation standard text, that means the station P1 has successfully updated the first ciphering key K1 (in this case, the second ciphering key K2) into the second ciphering key K2 (in this case, the third ciphering key K3), therefore, the follow up transmission data between the access point 34 and the station P1 is encrypted and decrypted by the second ciphering key K2 (in this case, the third ciphering key K3), therefore, continuously execute step 250. Moreover, Jordan also discloses this limitation on Figs. 10-11, Pars. 0088-0089] but does not specifically disclose **re-setting an out-of-sync counter to zero upon successful decryption**.

However, Loc discloses a method for detecting a security breach in a network wherein "Each time client 108 successfully decrypts a packet, the encryption failure counter is reset to zero" (Loc, Col. 6, lines 57-69).

Loc, Chen, and Jordan are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen-Jordan by re-setting an out-of-sync counter to zero upon successful decryption as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

Regarding claim 9, Chen-Jordan combination further discloses **the key synchronization system according to claim 8** but does not specifically disclose **wherein said at least one access point further maintains an out-of-sync counter to track the number of packets where decryption fails due to mismatched keys**.

However, Loc discloses a method for detecting a security breach in a network wherein "Each time client 108 fails to successfully decrypt a packet, the encryption failure counter is incremented" (Fig. 5, Col. 6, lines 59-61).

Loc, Chen, and Jordan are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen-Jordan by maintaining, by said at least one access point, an out-of-sync counter to track the number of packets where decryption fails due to mismatched keys as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

Regarding claim 14, Chen-Jordan-Loc combination further discloses **the method according to claim 3, wherein said out-of-sync counter comprises a predetermined threshold that if exceeded causes communication to terminate between the access point and a source of the data frames causing the threshold of said out-of-sync counter to be exceeded** as [Loc, Col. 6, lines 61-65: When the encryption failure counter reaches a predetermined threshold n (that is, when n consecutive failures have occurred) (step 512), client 108 sends an alert packet to access point. Loc, Col. 6, lines 5-9: furthermore, upon receiving the alert of a security breach, the access point "responds by immediately removing the MAC address of client 108 from its list of authorized clients, by ceasing to send any packets to the MAC address of client 108, and by discarding all packets that are received from the MAC address of client 108]

7. **Claims 5-6 and 10-12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen in view of Jordan and further in view of Kelem et al. US 6,118,869 (hereinafter "Kelem").

Regarding claim 5, Chen-Jordan combination discloses **the method according to claim 1** but does not specifically disclose **further comprising setting the old encryption key equal to a null value, said null value representing a no encryption mode**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen-Jordan by setting the old key equal to a null value, said null value representing a no encryption mode as described by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim 6, Chen-Jordan combination discloses **the method according to claim 1** but does not specifically disclose **further comprising setting the current encryption key and the old encryption key to a null value, said null value representing a no encryption mode**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen-Jordan by setting the current encryption key and the old encryption key to a null value, said null value representing a no encryption mode as taught by Kelem in order to modify the keys to provide a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim 10, Chen-Jordan combination discloses **the key synchronization system according to claim 8** but does not specifically disclose **wherein said at least one access point is configured for setting the old encryption key to a null value, said null value representing a no encryption mode**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen-Jordan by setting the old encryption key at the access point to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim 11, Chen-Jordan combination discloses **the key synchronization system according to claim 8** but does not specifically disclose **wherein said at least one access point is configured for setting the new encryption key to a null value, said null value representing a no encryption mode**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen-Jordan by setting the new encryption key at the access point to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim 12, Chen-Jordan combination discloses **the key synchronization system according to claim 8** but does not specifically disclose **wherein said at least one access point initially sets the old encryption key to a null value**.

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value

or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Chen and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Chen-Jordan by setting the old encryption key at the access point initially to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Conclusion

8. Examiner cites particular pages or columns or paragraphs and/or line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, applicant fully considers the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is

(571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/T N/
Examiner, Art Unit 2436